Software Assurance (SwA) Forum – Fall 2012

Emerging Software Assurance Initiatives

"Security | Quality | Reliability"

* *

Kevin E. Greene
Program Manager (SwA), Cyber Security Division
Homeland Security Advanced Research Projects Agency
Science & Technology Directorate
Department of Homeland Security
E: kevin.greene@hq.dhs.gov
O: 202-254-6877

* *

Homeland Security

Innovations and Advancements

DHS S&T continues with an aggressive cyber security research agenda

- Working with the community to **solve the cyber security problems** of our current (and future) infrastructure
- Working with **academia and industry** to improve research tools and datasets
- Looking at future R&D agendas with the **most impact** for the nation, including education

Software Assurance

Homeland Security

SBIR Work – Phase II

Homeland Security

Emerging Software Assurance Initiatives
"Security | Quality | Reliability"

SBIR SwA – Phase II efforts

Through the **DHS S&T SBIR Program**, **three Phase II** efforts were selected under this topic to provide solutions to *improve quality and reliability* of software used in the nation's critical infrastructures. These efforts will:

- Extend static analysis techniques for source code to allow them to systematically explore the platform space.
  - This will involve utilizing distributed build-and-test systems to harness the cloud, with centralized collation and presentation of analysis results. Existing technology transition channels will be leveraged to achieve maximum impact
- Provide flexible interface to ingest the results
- Produce an open source implementation of the framework for unified and consistent reporting of vulnerabilities.

Funded SwA Phase II SBIRs

Software Quality Improvements

GRAMMATECH

- CodeSonar improvements – parallel processing, computer clustering with **Metronome**
- Transition proof of concept to full capability- multiplatform program analysis and concolic analysis techniques

Model Driven Solutions
Where Business Meets Technology

KDM Analytics

COMPLETED

July 2012

- Integration of several open source tools into **TOIF** for consistent representation
- Consistent reporting and adoption, mapping of CWEs (normalization reference) – using SFP
- Creates shared view of the software under assessment among existing analysis tools
- Establish common protocol for exchanging vulnerability findings -- Wireshark and DNS Bind

TOIF Integration

APPLIED VISIONS
SecureDecisions DIVISION

- Framework for linking disparate testing and vulnerability analysis tools with deep analytics and analysis
- Visual analytics to prioritize weakness and simply analysis and remediation
- Leverages TOIF framework

CWEVIS

Homeland Security

Emerging Software Assurance Initiatives
"Security | Quality | Reliability"

New Developments

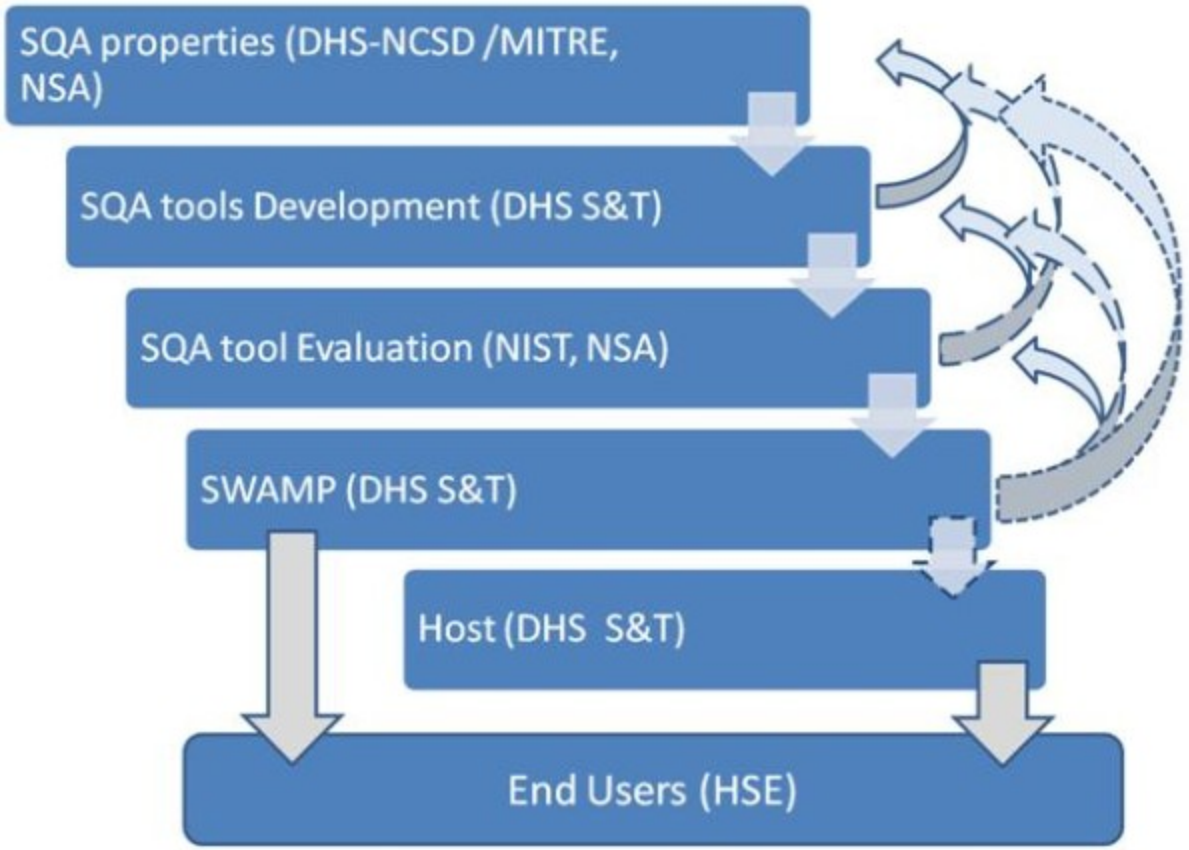
Homeland Security

Emerging Software Assurance Initiatives
"Security | Quality | Reliability"

Announcements

- By end of the month, **Broad Agency Announcement (BAA)** awards will be finalized and performers will be announced
- Principal Investigator - **PI Meeting and Kick-Off**, Oct. 9th- 11th (***limited to government only***)
- Official release of **– proposal abstracts and PI meeting presentations**
- Upcoming Press Release to announce performers

Program-Level Approach to SwA



Software Quality Assurance (TTA-1)

25 Proposals submitted, 3 performers selected

Software Quality Assurance (SQA)

Where are we???

- Protect the nation's critical infrastructure (energy, transportation, banking, telecommunications, finance, and others) – **"having kept pace"**
- The cost of failures is staggering – **over $60 million**
- Threats must be addressed throughout the software development lifecycle – **"1-10-100 Quality Cost Rule"**
- Need innovation and breakthroughs in testing and evaluation of software – need better tools

Software Assurance Marketplace – TTA-14

6 Proposals submitted, 1 performer selected

Homeland Security

Emerging Software Assurance Initiatives
"Security | Quality | Reliability"

SWAMP Focus Area

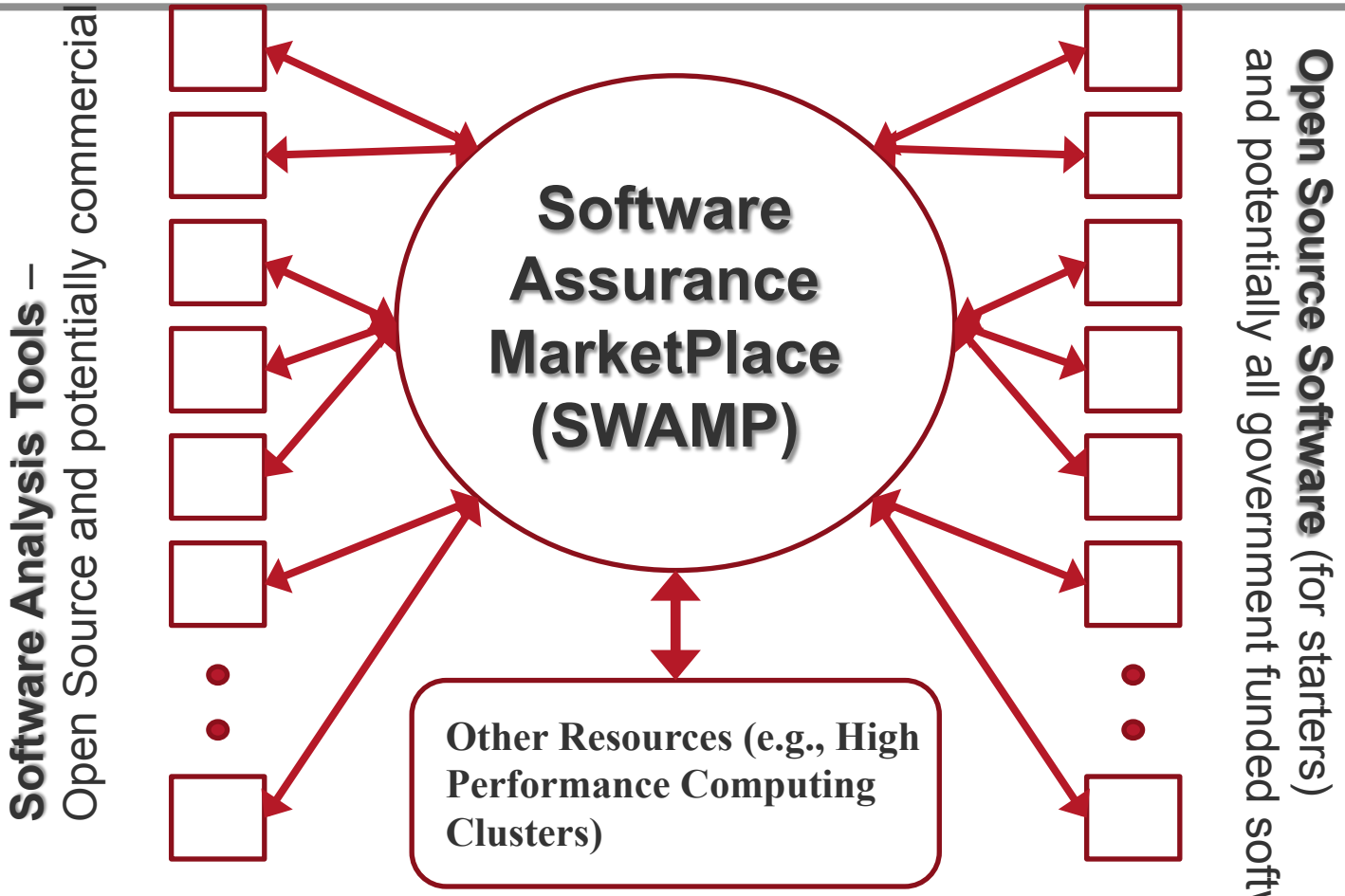
- Focuses on the research infrastructure necessary to enable software quality assurance and related activities
- A software assurance facility and the associated research infrastructure services that will be made available to both software analysis researchers and software developers, both open source and proprietary
- DHS expects the SWAMP to become a national level R&D resource in software assurance for open security technologies, used across civilian agencies and their communities as both a research platform and core component supporting US Government supported software development activities

Homeland Security

SwA Research Infrastructure

- Develop a research infrastructure to enable open source code developers and software analysis researchers access to new and existing analysis tools and testing techniques
- Capability to provide a **rich ecosystem of SwA tools** and software packages to validate software is secure and resilient.
- Build knowledge base schemas and results repositories for advancements in software improvements.
- High performance resilient computing platform with integrated identity management services for secure access management

SWAMP Conceptual Architecture



An Initial Operating capability (IOC) for this system is expected within 15 months of the start of activities

Homeland Security

Initial Operating Capability

What we expect to see!! --- Notionally:

- 5 Software Analysis (SwA) tools running against 100 software packages with multiplatform support.
- Analysis workflows and merged tool reports.
- Authenticated web access with training materials and 24/7 Network Operations Center (NOC)
- 528 CPU cores, 150TB storage, redundant network connectivity

Technical Topic Areas (TTA)

TTA-1
Software Quality Assurance

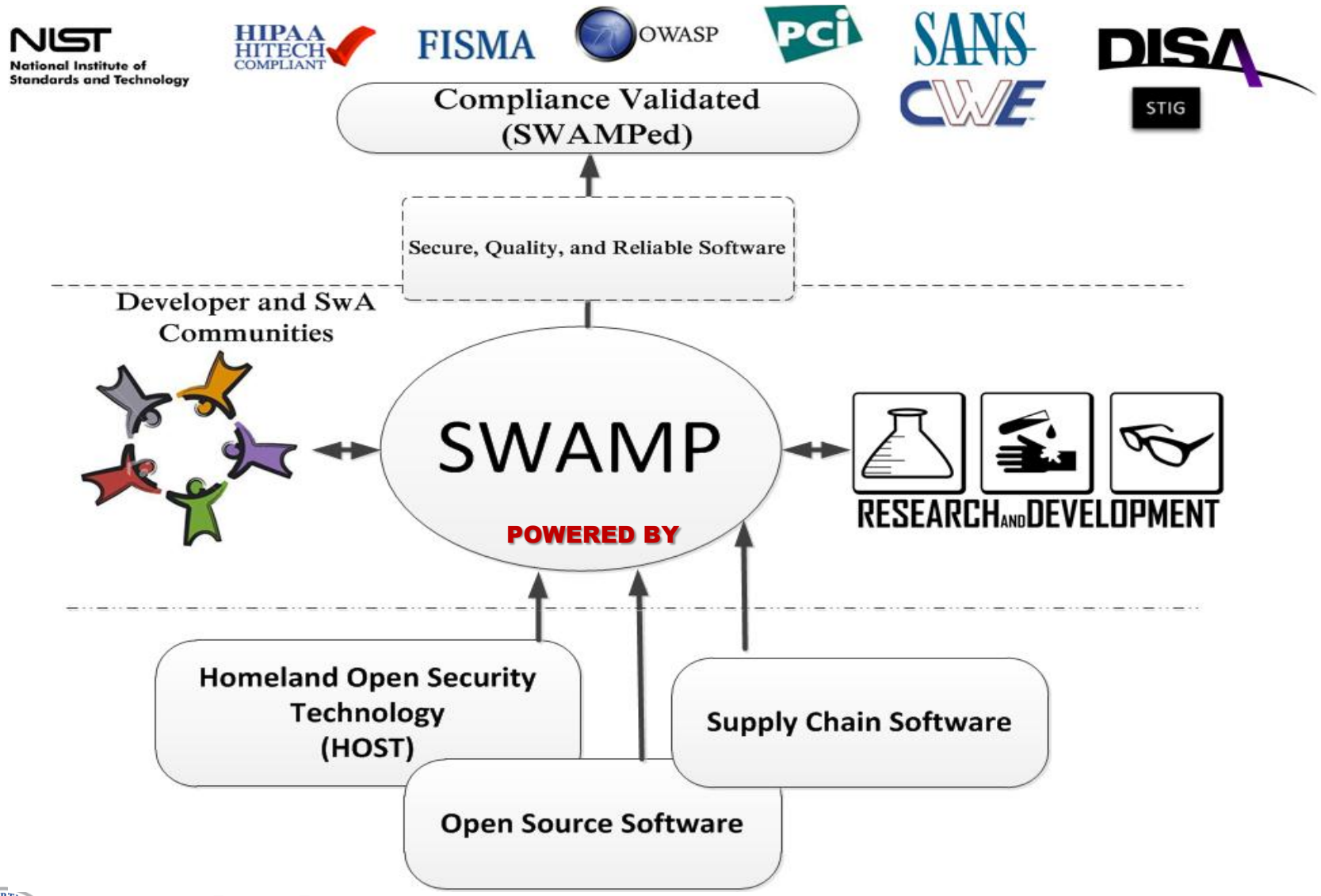
- Improved methods and techniques for evaluating and testing software
  - Advancements in proof-carrying code techniques for "trustworthiness"
  - Focused on reducing false-positive rates – combined IFA and run-time monitoring
- Establish "Gold Standard" for measuring effectiveness of SwA tools
  - Measurements for all SwA used in SWAMP
  - Establish "Ground Truth" – reduction in false-negative rate
  - Mathematically prove code locations are safe
- Rich Visual Analytics and correlation engine
  - Simplify and prioritize analysis to speed remediation process
  - Correlates dynamic and static analysis for detailed vulnerability detection
  - Detailed workflow analysis to model threats and exposures

TTA-14
Software Assurance Marketplace (SWAMP)

- Research infrastructure to provide advances in new forms of software analysis and testing
- Analyses to run in reliable and repeatable workflows
- On-demand access to extendable computing resources
- Platform to integrate dynamic and static analysis and testing
- Tool isolation

Homeland Security

Synergistic Capabilities



Homeland Security

Emerging Software Assurance Initiatives
"Security | Quality | Reliability"

Follow-up

Kevin E. Greene
Program Manager (SwA), Cyber Security Division
Homeland Security Advanced Research Projects Agency
Science & Technology Directorate
Department of Homeland Security
E: kevin.greene@hq.dhs.gov
O: 202-254-6877

For more information, visit

http://

www.cyber.st.dhs.gov

Homeland Security

Emerging Software Assurance Initiatives
"Security | Quality | Reliability"